wiley

ALERT

NIST Releases Version 1.1 of its Cybersecurity Framework with Important Changes

April 17, 2018

On April 16, 2018, the National Institute of Standards and Technology (NIST) released an updated version of its Framework for Improving Critical Infrastructure Cybersecurity (Framework). The Framework Version 1.1 is intended to refine, clarify, and enhance the original Framework Version 1.0 released in February 2014. The Framework is voluntary guidance to guide cybersecurity activities and help organizations manage cybersecurity risks. While the Framework was developed to improve cybersecurity risk management in critical infrastructure, the Framework can be used by organizations in any sector or community.

Companies have been using the Framework for years in various ways. U.S. agencies use it, and international regulators look to and build their approaches on it. As a result, many urged NIST not to make major structural changes to the Framework, lest it foster fragmentation on cybersecurity best practices. Industry commenters filed several rounds of comments and participated in meetings with NIST as the revisions were considered. The new Version addresses many of those comments and retained some of the more substantial additions, like vulnerability disclosure programs and supply chain protocols. It also explicitly addresses the Internet of Things.

Overall, Version 1.1 wisely retains the core features that made the original Framework a success. NIST emphasizes throughout Version 1.1 that there are a variety of ways to use the Framework and the decision about how to apply it is left to the implementing organization. The update clarifies that "compliance with the Framework" will have different meanings to different stakeholders, and that the Framework has utility as a structure and language for organizing cyber activities.

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Practice Areas

Privacy, Cyber & Data Governance
Telecom, Media & Technology

Version 1.1 makes several key updates, including:

- Updating the scope of technologies covered by the Framework, noting that the Framework is applicable to organizations relying on technology, whether their cybersecurity focus is primarily on "information technology (IT), industrial control systems (ICS), cyber-physical systems (CPS), or connected devices more generally, including the Internet of Things (IoT)."
- Adding language to Section 2.2 to better explain how to use Framework Tiers in Framework implementation.
- Creating a new Subcategory related to the vulnerability disclosure lifecycle. There are increasing expectations for companies to have methods to identify and manage vulnerabilities. These may not be right for all companies, but with the addition to NIST's Framework, they are something prudent companies should consider.
- Greatly expanding Section 3.3 to add discussion of supply chain risk management (SCRM). NIST emphasizes communication among stakeholders up and down supply chains, identifies examples of cyber SCRM activities, and notes that cyber SCRM encompasses technology suppliers and buyers as well as non-technology suppliers and buyers. The update also adds a Supply Chain Risk Management Category to the Framework Core.
- Discussing "Buying Decisions" in a new Section 3.4, defining the objective as making the best buying decision among multiple suppliers, given a carefully determined list of cybersecurity requirements.
- Adding a new Section 4.0, "Self-Assessing Cybersecurity Risk with the Framework," describing how to use the Framework for self-assessing and demonstrating cybersecurity through measurements. NIST notes that the development of cybersecurity performance metrics is evolving and encourages organizations to innovate and customize how they incorporate measurements.
- Refining the language of the Access Control Category to better account for authentication, authorization, and identify proofing.

NIST will be holding a webcast discussing how the Framework was developed, describing the Framework's basic concepts, demonstrating how the Framework can be used by organizations, and highlighting the recent updates on April 27, 2018.

NIST has underway numerous other efforts that will affect the informative references in the Framework, and the tools for private sector companies. As those efforts unfold, organizations should consider adapting their approaches to stay up to speed with changing expectations.

Wiley Rein has been actively involved in shaping the original and new Frameworks and helps clients across industries use and adapt it. We have also urged other countries to model their private sector cybersecurity strategies on it, in lieu of prescriptive regulation. We are actively engaged on other NIST publications and work, as the agency continues to produce guidance on everything from IoT to privacy engineering.

Megan Brown serves on the U.S. Chamber of Commerce's Cybersecurity Leadership Council and is a Visiting Fellow at the National Security Institute at George Mason's Antonin Scalia Law School. She has guest lectured at American University School of Law on the application of the NIST Framework and corporate governance.

Matt Gardner and Megan Brown have been recognized among the nation's top Cybersecurity & Data Privacy "Trailblazers" by The National Law Journal.

Katy Ross advises technology companies on a variety of issues, including regulatory compliance and enforcement actions. She has helped tech companies with security policies and agency investigations.